15. Ilmenauer TK-Manager Workshop
Technische Universität Ilmenau, 17. Mai 2019
DOI: 10.22032/dbt.38489
URN: urn:nbn:de:gbv:ilm1-2019200270

Warum wir mehr Bommelmützen brauchen – Muss sich die Sicherheit im Cloud DataCenter jetzt warm anziehen?

von Dipl.-Phys. Christoph Schmidt

Christoph Schmidt ist seit 2005 bei der Controlware GmbH als Security Consultant tätig. Nach dem Studium der Physik an der TH Darmstadt waren weitere Stationen im Beruf die Netzwerkadministration beim Hessischen Rundfunk in Frankfurt/M., sowie div. IT Dienstleister mit dem Schwerpunkt der IT Security. Neben den klassischen Themen wie z.B. Netzwerksecurity oder auch „Network Access Control" beschäftigt sich Christoph Schmidt mit dem Thema „Data Center oft the Future", welches Unternehmen durch die Einführung von Virtualisierung bzw. „Cloudifizierung" vor neue Herausforderungen stellt. Seit geraumer Zeit spielt „Cloud Security" in allen Facetten eine große Rolle bei Beratungs- und Umsetzungsdienstleistungen.Ebenso bedingen neuartige Angriffsmethoden oftmals ein Re-Design von Netzwerkinfrastrukturen in Bezug auf Segmentierung und DMZ/Internet/Cloud-Übergängen.

DOI: 10.22032/dbt.38495

Warum wir mehr Bommelmützen brauchen – Muss sich die Sicherheit im Cloud DataCenter jetzt warm anziehen?"

In diesem Vortrag werden Konzepte zur Umsetzung von Netzwerkarchitekturen in cloud-basierten Data Centern beschrieben.

Klassische auf Routing- und Switchingtechnologien basierende Data Center erfahren in der Cloud bzw. in einem Rechenzentrum, welches auch einer Software-Defined-Technologie basiert, einen komplett neuen Ansatz.

Bisherige, durch eine 3-tier Architektur im Switchingumfeld gebaute Rechenzentren werden durch eine Software-Defined-Network Architektur abgelöst. Hierbei wird die Hardware von der eigentlichen Funktion (Software) entkoppelt.

An den Stellen, an denen früher das Netzwerk im Vordergrund stand und somit auch die Sicherheitswirkprinzipien hier ansetzten, gilt im modernen Data Center ein sogenannter applikationszentrischer Ansatz.

Dem einhergehend werden auch Sicherheitsmaßnahmen in ihrer Implementation einer Revision unterzogen, d.h. eine klassische Sicherheitsarchitektur muss in der Cloud ganz anders „gebaut“ werden.

Fazit

Ein (Cloud) Data Center ist lange schon kein Märchen mehr. Ein Umdenken bei der Verkehrsflusssteuerung und der Umsetzung von Sicherheitsrichtlinien ist die Basis für den sicheren Betrieb einer modernen Data Center Architektur. Wichtig ist aber, dass sich die eigentlichen Security-Policies und –Wirk-prinzipien hierbei nicht ändern.